

English Abstract

23oct07 13:16:00 User266881 Session D3185.2
Sub account: 42933/306360

SYSTEM:OS - DIALOG OneSearch

File 345:Inpadoc/Fam.& Legal Stat 1968-2007/UD=200741

(c) 2007 EPO

*File 345: August 27, 2007 - reloaded with new and enhanced content.

See HELP NEWS 345 for details.

File 351:Derwent WPI 1963-2007/UD=200767

(c) 2007 The Thomson Corporation

Set	Items	Description
-----	-------	-------------

---	-----	-----
S1	2	PN=JP 11282804

1/5/2 (Item 1 from file: 351)

DIALOG(R) File 351:Derwent WPI

(c) 2007 The Thomson Corporation. All rts. reserv.

0009719520 - Drawing available

WPI ACC NO: 2000-004219/ 20 00 01

XRPX Acc No: N2000-003665

User authentication system for client-server system connected to internet -
transmits completed authentication information to client when user
authentication is successful

Patent Assignee: SECOM JOHO SYSTEM KK (SECO-N)

Inventor: HIRAI S

Patent Family (1 patents, 1 countries)

Patent	Application
--------	-------------

Number	Kind	Date	Number	Kind	Date	Update
JP 11282804	A	19991015	JP 199885319	A	19980331	200001 B

Priority Applications (no., kind, date): JP 199885319 A 19980331

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing	Notes
JP 11282804	A	JA	11		6	

Alerting Abstract JP A

NOVELTY - When receiving access from a client (12) which is not finished the user authentication, a redirect demand information is transmitted for accessing web authentication server (16) to perform user authentication of client. When the user authentication is successful, a completed authentication information indicating that user authentication of client is successful, is transmitted. DETAILED DESCRIPTION - When completed authentication information is transmitted to client, a redirect demand information for accessing web service server (10) collectively is transmitted. An INDEPENDENT CLAIM is also included for the user authentication procedure.

USE - For client-server system connected to internet.

ADVANTAGE - As user authentication is performed directly between client and authentication server, interdependence relationship of web service server and authentication server is reduced, hence versatility of authentication server is enhanced with simple authentication system.

DESCRIPTION OF DRAWING(S) - The figure shows schematic component of

communication system. (10) Web service server; (12) Client; (16)
Authentication server.

Title Terms/Index Terms/Additional Words: USER; AUTHENTICITY; SYSTEM;
CLIENT; SERVE; CONNECT; TRANSMIT; COMPLETE; INFORMATION; SUCCESS

Class Codes

International Classification (Main): G06F-015/00
(Additional/Secondary): H04L-012/54, H04L-012/58, H04L-009/32

File Segment: EPI;

DWPI Class: T01; W01

Manual Codes (EPI/S-X): T01-J; W01-A03B; W01-A05B; W01-A06G2

53976375 Family ID: 23976376

Patent Family:		Kd Date	Applic No	Kd Date	Wk Added
Patent No	JP 11282804	A	19991015	JP 199885319	A 19980331 199948 (B)
Priority Data (No, Kind, Date):					
	JP 199885319	A	19980331		

JAPAN (JP) PATENT(S) :

```

v. 6 main: G06F-015/00
v. 6      : H04L-009/32
v. 6      : H04L-012/54
v. 6      : H04L-012/58
v. 8 adv : G06F-0015/00
v. 8 adv : G06F-0021/20
v. 8 adv : H04L-0009/32
v. 8 adv : H04L-0012/54
v. 8 adv : H04L-0012/58
v. 8 core: G06F-0015/00
v. 8 core: G06F-0021/20
v. 8 core: H04L-0009/32
v. 8 core: H04L-0012/54
v. 8 core: H04L-0012/58
A I      R 20060101 20051110 M EP
A I F R 20060101 20051220 M JP
A I L R 20060101 20051220 M JP
A I      R 20060101 20051110 M EP
A I      R 20060101 20051110 M EP
C I      R 20060101 20051110 M EP
C I F R 20060101 20051220 M JP
C I L R 20060101 20051220 M JP
C I      R 20060101 20051110 M EP
C I      R 20060101 20051110 M EP

```

- 3 -

特開平11-282804

(43) 公開日 平成11年(1999)10月15日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
12/54			6 7 5 D
12/58		11/20	1 0 1 B

審査請求 未請求 請求項の数 5 O L (全 11 頁)

(21) 出願番号 特願平10-85319

(22) 出願日 平成10年(1998) 3 月31 日

(71) 出願人 596143657

セコム情報システム株式会社
東京都三鷹市下連雀 8 丁目10番16号 セコム情報システム株式会社内

(72) 発明者 平井 滋

東京都三鷹市下連雀 8 - 10 - 16 セコム情報システム株式会社内

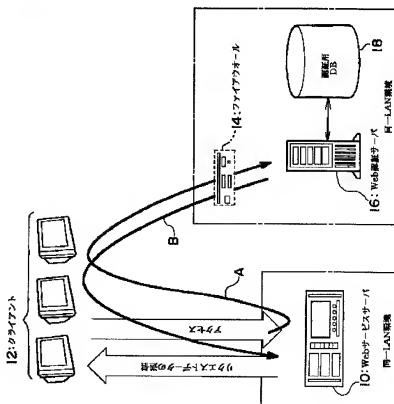
(74) 代理人 弁理士 吉田 研二 (外 2 名)

(54) 【発明の名称】 ユーザ認証機能付き通信システム及びユーザ認証方法

(57) 【要約】

【課題】 サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで共通利用することが容易な認証システムを提供する。

【解決手段】 ユーザ認証を終えていないクライアント12からアクセスを受けた場合、Web認証サーバ16にアクセスしてユーザ認証を済ませるよう、リダイレクト要求を含むWebページをクライアント12に返信する。クライアント12がこれを受けてWeb認証サーバ16にアクセスすれば、該Web認証サーバ16では必要な認証処理を行い、認証に成功すればその旨をクッキーに設定してクライアント12に所定Webページを返信する。この際、このWebページに再度Webサービスサーバ10にアクセスさせるためのリダイレクト要求を含めてもよい。こうすれば、Webサービスサーバ10とWeb認証サーバ16との直接のアクセスを無くして、Web認証サーバ16の独立性、汎用性を高めることができる。



【特許請求の範囲】

【請求項 1】 ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて、

前記サービスサーバは、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信する手段を含み、前記認証サーバは、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す認証済み情報を前記クライアントに送信する手段を含む、

ことを特徴とする通信システム。

【請求項 2】 請求項 1 に記載の通信システムにおいて、

前記認証サーバに含まれる前記手段は、前記認証済み情報を前記クライアントに送信する際に、併せて前記サービスサーバにアクセスするよう要求するリダイレクト要求情報を送信する、ことを特徴とする通信システム。

【請求項 3】 請求項 1 又は 2 に記載の通信システムにおいて、

前記クライアントは、前記サービスサーバ又は前記認証サーバからリダイレクト要求情報を受信した場合に前記サービスサーバ又は前記認証サーバにアクセスする手段を含むことを特徴とする通信システム。

【請求項 4】 請求項 1 乃至 3 のいずれかに記載の通信システムにおいて、

前記クライアントは、前記認証サーバから既に前記認証済み情報を受信している場合に、前記サービスサーバへのアクセスの際に前記認証済み情報を該サービスサーバに送信する手段をさらに含むことを特徴とする通信システム。

【請求項 5】 ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて前記クライアントのユーザ認証を行う方法であって、

前記サービスサーバにて、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信し、前記認証サーバにて、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す情報を前記クライアントに送信する、ことを特徴とするユーザ認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はユーザ認証機能付き通信システム及びユーザ認証方法に関し、特に、ネット

ワークに接続されたクライアント／サーバ間でのユーザ認証において認証サーバの汎用性を高める技術に関する。

【0002】

【従来の技術】 近年、ワールドワイドウェブ (WWW) を用いる通信環境が急速に普及しており、単なる学術レベルでの利用のみならず、オンラインショッピングや商用データベースサーバ等、商業利用もまた急速に普及している。そして、このように WWW を本格的に商業利用するには、Web サーバ側で信頼性の高いクライアントのユーザ認証を行う技術を確立することが必須であり、このため各種の技術が提案されている。

【0003】 図 6 は、WWW における従来一般的に考えられる認証サーバを持ったサービスサーバのクライアントの認証の仕組みを説明する図である。同図に示すように、WWW では、Web ブラウザを搭載したクライアント 100 はインターネットに URL (Uniform Resource Locator) を送出することにより、該 URL により特定されるリソース (ハイパーテキスト) を取得し、ディスプレイ上至望の画像表示を得ることができ、

【0004】 この際、クライアント 100 が URL により特定したリソースが、Web サービスサーバ 102 に格納されているものであり、ユーザ認証を必要とするサービスに関するものであれば、該 Web サービスサーバ 102 はユーザ ID やパスワード等の認証情報を求めるハイパーテキストをクライアント 100 に送る。そして、これに応じてクライアント 100 は所定の認証情報を該 Web サービスサーバ 102 に送信する。

【0005】 こうして、クライアント 100 から認証情報を受け取った Web サービスサーバ 102 は、専用のアプリケーションインタフェース (API) を使い、通常は同一ドメイン、すなわち同一 LAN 環境に設置される認証サーバ 104 に対し、その受け取った認証情報を転送するとともに、ユーザ認証処理を依頼する。この依頼を受けた認証サーバ 104 は認証用データベース 106 に格納された各種認証情報を参照しつつユーザ認証を行う。そして、認証に成功して正規のユーザであると確認されれば、Web サービスサーバ 102 とクライアント 100 とのその後の通信に供するよう、当該クライアント 100 がユーザ認証済みであることを表すクッキー (Cookie) を発行する。このクッキーは、Web サービスサーバ 102 からのハイパーテキストの返信に際して、そのヘッダ部分に含められる情報であり、以後、所定内容のクッキーを保持しているクライアント 100 からのアクセスに対しては、Web サービスサーバ 102 は既にユーザ認証を終えているクライアント 100 からのアクセスであると判断し、認証サーバ 104 でのユーザ認証を改めて行うことなく、ユーザ所望のハイパーテキストをクライアント 100 に返信する。

【0006】

【発明が解決しようとする課題】以上説明した従来一般のユーザ認証技術によれば、クライアント100から送信された認証情報をもとにユーザ認証を行うことができ、WWWの商業利用に際して必要十分なセキュリティを確保することが可能となる。

【0007】しかしながら、上記従来技術によれば、認証サーバ104がWebサーバとして構築されたものではなく、フロントエンドとして用いられるWebサーバ102とバックエンドとして用いられる認証サーバ104とが深い依存関係を必要とし、認証の依頼と結果通知のための専用のソフトウェアが両者にインストールされることが多い。このため、たとえ高機能な認証サーバ104を構築したとしても、これを他のWebサーバ等で利用することは困難であり、認証サーバ104を複数のサービスで共通利用する効率的なシステムの構築が困難であった。

【0008】本発明は上記課題に鑑みてなされたものであって、その目的は、サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで共通利用することが容易な認証システムを提供することにある。

【0009】

【課題を解決するための手段】(1)上記課題を解決するために、本発明は、ネットワーク上に相互に通信可能に接続されたサービスサーバ、認証サーバ、及びクライアントを含むシステムにおいて、前記サービスサーバは、必要なユーザ認証を終えていない前記クライアントからアクセスを受けた場合に、該クライアントに対して前記認証サーバにアクセスするよう要求するリダイレクト要求情報を送信する手段を含み、前記認証サーバは、前記クライアントからアクセスがあった場合に該クライアントのユーザ認証を行い、前記ユーザ認証が成功した場合にユーザ認証が成功したことを表す情報を前記クライアントに送信する手段を含む。

【0010】(2)また、本発明の一態様では、前記認証サーバに含まれる前記手段は、ユーザ認証が成功したことを表す前記情報を前記クライアントに送信する際に、併せて前記サービスサーバにアクセスするよう要求するリダイレクト要求情報を送信する。

【0011】(3)また、本発明のさらに他の態様では、前記クライアントは、前記サービスサーバ又は前記認証サーバからリダイレクト要求情報を受信した場合に前記認証サーバ又は前記サービスサーバにアクセスする手段を含む。

【0012】(4)さらに、本発明の他の態様では、前記クライアントは、前記認証サーバから既に前記認証済み情報を受信している場合に、前記サービスサーバへのアクセスの際に前記認証済み情報を該サービスサーバに送信する手段をさらに含む。

【0013】

【発明の実施の形態】以下、本発明の実施の形態について図面に基づき詳細に説明する。

【0014】図1は、本発明の実施の形態に係る認証システムの概略を説明する図である。同図において、Webシステムは、インターネット上に接続されたWebサーバ10及びクライアント12と、同じくインターネットにファイアウォール14を介して接続されたWeb認証サーバ16と、を含んで構成されており、Webサーバ10とクライアント12とWeb認証サーバ16は相互に通信可能に接続されている。また、Web認証サーバ16は同一LAN環境に設置された認証用データベース18にアクセスすることができるようになっている。

【0015】同図に示すWebシステムにおいて、Webブラウザを搭載したクライアント12が未だ有効なユーザ認証を済ませていないWebサーバ10にアクセスした場合、該Webサーバ10はクライアント12に対しリダイレクト要求を含むWebページを送信し、Web認証サーバ16に改めてアクセスするように要求する。クライアント12はこのリダイレクト要求を解釈し、図中矢印Aに示すようにして、ユーザの干渉なしにWeb認証サーバ16に自動的にアクセスする。

【0016】多くのWebブラウザには、「リダイレクト要求」が含まれるハイパーテキストを受信した場合に、その要求を解釈して指定Webページを自動的にリロードすることができるようになっており、本認証システムではこの機能を積極活用することによって、Webサーバ10とWeb認証サーバ16との直接的な通信を廃し、Web認証サーバ16の汎用性を高めることに成功している。

【0017】その後、矢印Aに示すようにして、クライアント12がWebサーバ10の要求をリダイレクトしてWeb認証サーバ16にアクセスすれば、Web認証サーバ16は認証用データベース18に照らし合わせてユーザ認証を行う。

【0018】ここでWeb認証サーバ16にてユーザ認証に成功すれば、該Web認証サーバ16はクライアント12に対してさらに別のリダイレクト要求を含むWebページを送信し、今度はWebサーバ10に改めてアクセスするように要求する。この際、このWebページにおいてはユーザ認証済みの旨を示す情報がクッキーに設定される。そして、このクッキーの内容を含んだURLをWebサーバ10が受け取ることににより、Webサーバ10はユーザが希望するWebページをクライアント12に送信する。

【0019】本認証システムにおいてはWebサーバ10からWeb認証サーバ16へ直接のアクセスが発生しないため、それらWebサーバ10とWeb認証サーバ16との間のインターフェースを非常

に簡潔なものとすることができる。これにより、サービスサーバと認証サーバとの独立性及び汎用性を高め、認証サーバを複数のサービスで容易に共通利用することができる。

【0020】また、本認証システムでは、Web認証サーバ16及びWebサービスサーバ10はいずれもインターネット上でIPアクセス可能なよう設置されていればよく、例えばWeb認証サーバ16にはファイアウォール14を介する以外に外部からアクセスできないようにしてもよい。さらに、Web認証サーバ16とWebサービスサーバ10は従来技術のように必ずしも同一LAN環境に設置する必要がない。このため、同じインターネット上でIPアクセス可能なよう設置された他のWebサービスサーバ10からもまた、同Web認証サーバ16に対して容易にユーザ認証を依頼することができる。

【0021】以下、本認証システムの構成及び認証手順についてさらに詳細に説明する。

【0022】図2は、Webサービスサーバ10の構成を本通信システムの全体構成とともに示す図である。同図に示すように、Webサービスサーバ10は、httpd (Hyper Text Transfer Protocol Daemon) 20と、ファイル記憶部22と、を有しており、httpd 20には、データ受信部24、データ解析部26、データ処理部28、30、データ送信部32、httpd設定ファイル34が設けられている。ここで、データ記憶部24、データ解析部26、データ処理部28、データ送信部32、ファイル受信部22は従来一般のWebサーバに設けられているものと同様であり、データ処理部30とhttpd設定ファイル34とが本実施の形態に係る認証システムを実現するために新たに追加された構成である。また、ファイル記憶部22にはサービス内容たるWebページの他、ユーザ認証に失敗した旨を通知するための認証失敗ページに関するファイルが格納されている。また、データ処理部28はhttpd設定ファイル34での設定により特に起動される実行モジュールであり、httpヘッダの解析による従来一般のアクセス可否チェックを第1段階のセキュリティチェック機能として実現するとともに、第2段階のセキュリティチェック機能としてクライアント12から受け取るクッキーの内容を基にしたアクセス可否チェックを行う。

【0023】次に、図3はWeb認証サーバ16の構成を示す図である。同図において、Web認証サーバ16の大部分の構成はWebサービスサーバ10と同様であり、対応する構成には対応符号を付している。Web認証サーバ16には特に認証用データベース18が接続されており、データ処理部30aは受信したURLが認証を要求するものである場合に該認証用データベース18に問い合わせることによりユーザ認証を行うことができるようになっていく。

【0024】本認証システムでは、まず、図2に示すWebサービスサーバ10において、クライアントから送信されたURLがデータ受信部24により受信され、Webサービスサーバ10のデータ解析部26は受信したURLから要求されているファイルの名称や各種変数等を取得する。その後、通常ならばデータ処理部28によってサービス内容たる所定ファイルがファイル記憶部22から読み出され、それが必要に応じて加工され、データ送信部32によってインターネットに送出されるところ、本Webサービスサーバ10では、httpd設定ファイル34によってデータ処理部30が起動指定されており、該データ処理部30によって2段階のアクセス可否チェックが施される。

【0025】すなわち、データ処理部30では、まず第1段階のアクセス可否チェックとしてhttpヘッダの解析が行われ、URLが一定範囲のIPアドレスから送信されたものであるのか、たとえばjpドメインを有するクライアントからの要求であるか等の事項がチェックされる。そして、ここでのチェックに適合しない場合には認証失敗の旨を表すWebページがクライアント12に返信される。

【0026】一方、このチェックに適合する場合、さらに第2段階のアクセス可否チェックが行われ、クライアント12から受信するデータにクッキーが含まれているか、含まれているとして内容はどのようなものかが確認される。すなわち、本認証システムではWeb認証サーバ16によって正常にユーザ認証が行われているクライアント12に対してはユーザ認証済みの旨を表すクッキーが発行されるようになっており、ユーザ認証済みのクライアント12からのアクセスに際してはそのクッキーがWebサービスサーバ10に送信されるようになっていく。

【0027】そして、Webサービスサーバ10ではクライアント12からアクセスがあった場合に第2段階のアクセス可否チェックとしてそこから送信されてくるクッキーの内容を確認する。この確認によってユーザ認証済みの旨のクッキーを伴うアクセスであると判れば、クライアント12に要求されたWebページを正常に返信する。一方、ユーザ認証済みの旨のクッキーを伴わないアクセスであると判れば、クライアント12にMETAタグ付きのWebページを送信するなどのリダイレクト要求を行う。このMETAタグとはクライアント12に対するリダイレクト要求情報のうちの1つであり、たとえば「<META HTTP-EQUIV="Refresh" CONTENT="3; URL=Web認証サーバ16中の認証要求.html">」のような形式を有する。この例では、該要求がクライアント12に到着してから3秒後にWeb認証サーバ16に格納されている「認証要求.html」がアクセスされる。

【0028】次に、図3に示すWeb認証サーバ16においては、クライアント12からリダイレクトして送信

されたURLがデータ受信部24aにより受け付けられ、データ解析部26aが受信したURLから要求されているファイルの名称や各種変数等を取得する。そして、クライアント12からのアクセスが認証要求.htmlに対するものであれば、Webサービスサーバ10と同様、データ処理部30aは、まず第1段階のアクセス可否チェックとしてhttpヘッダの解析を行い、このチェックに適合しないアクセスに対しては、認証失敗の旨を表すWebページをWebサービスサーバ10から取得するよう要求するMETAタグを付したWebページをクライアント12に送信する。このMETAタグは、たとえば「<META HTTP-EQUIV="Refresh" CONTENT="3; URL=Webサービスサーバ10中の「認証失敗.html」>」のような形式を有する。なお、この例では、該要求がクライアント12に到着してから3秒後にWebサービスサーバ10に格納されている「認証失敗.html」がアクセスされる。

【0029】一方、第1段階のアクセス可否チェックをクリアした場合には、さらにデータ処理部30aはクライアント12のユーザ認証を行う。ユーザ認証の方法はたとえばWeb認証サーバ16がクライアント12からユーザIDやパスワード等の認証情報を送信するよう要求してもよいし、また、Webサービスサーバ10側で予めクライアント12から所定の認証情報を受信しておく、それをクッキーヘッダに設定するなどの方法によりWebサービスサーバ10からWeb認証サーバ16へのリダイレクト要求によりクライアント12を介してWeb認証サーバ16に転送するようにしてもよい。Web認証サーバ16のデータ処理部30ではこうして得られる認証情報を基に適宜認証用データベース18に問い合わせることにより、ユーザ認証を行う。

【0030】そして、ユーザ認証に失敗すれば、データ処理部30aは、Webサービスサーバ10に格納されている認証失敗の旨を表すWebページにアクセスするよう、所定のURLをファイル格納部から読み出し、クライアント12にそのURLへのリダイレクト要求を行うWebページを送信する。一方、ユーザ認証に成功すれば、データ処理部30は、Webサービスサーバ10に格納されている所定Webページにアクセスするよう、所定のURLをファイル格納部から読み出し、クライアント12にそのURLへのリダイレクト要求を行うWebページを送信する。この際、この送信するWebページのヘッダにおいてはユーザ認証済みの旨を表すクッキーが設定される。

【0031】こうすれば、この後クライアント12がWebサービスサーバ10にアクセスする場合には、ユーザ認証済みの旨を表すクッキーが併せて送信されることになり、改めてユーザ認証を行うことなく、クライアント12のユーザは所望のWebページを正常にWebサービスサーバ10から受け取ることができる。

【0032】ここで、Webサービスサーバ10からWeb認証サーバ16への問い合わせが発生するケースについて、図4に示す通信シーケンス図に基づいて認証手順を説明する。

【0033】まず、クライアント12のユーザがWebサービスサーバ10に対するサービスを要求するURLを入力すれば(S101)、クライアント12にてそのURLをインターネットに送出する(S102)。その後、Webサービスサーバ10にてアクセス可否の確認が行われる(S103)。そして、上述した第2段階でのアクセス可否チェックにおいて、クライアント10からのアクセス要求が必要なクッキーを備えないものであると判断された場合は特に、Webサービスサーバ10からクライアント12にリダイレクト要求を含むWebページが送信される(S104)。

【0034】これを受けてクライアント12は、そのリダイレクト要求に従ってURLをインターネットに送出し、Web認証サーバ16にアクセスする(S105)。Web認証サーバ16では、上述した第1段階のアクセス可否チェックを行うとともに、ユーザ認証を行う(S106)。

【0035】そして、ユーザ認証に成功すれば、認証済みの旨の情報をクッキーに設定し、再びWebサービスサーバ10にアクセスするようリダイレクト要求を含むWebページをクライアント12に送信する(S107)。この際、ユーザ認証に失敗した場合は、ユーザ認証に失敗した旨を表す情報をクッキーに設定して所定のWebページをクライアント12に返信するようにしてもよい。こうすれば、たとえばWebサービスサーバ10にてユーザ認証に失敗したクライアント12からのアクセスを速やかに判別することができる。

【0036】その後、クライアント12ではWeb認証サーバ16から受信したWebページに含まれているリダイレクト要求に従い、再びWebサービスサーバ10にアクセスする(S108)。このアクセスではクライアントから送信されるURLに認証済みの旨のクッキーが含まれており、Webサービスサーバ10はユーザ認証を正規に終了したクライアントからのアクセスであると判断し(S109)、ユーザ所望のWebページをクライアント12に送信する(S110)。そして、クライアント12では受信したWebページを解釈してディスプレイ表示を行う。

【0037】なお、上述のように、ユーザ認証に失敗した旨のクッキーをWeb認証サーバ16で設定するようになった場合には、Webサービスサーバ10は、S110において、かかるクッキーを伴うアクセスに対しアクセス拒否の旨のWebページ等を返信するようにしてもよい。

【0038】また、以上のようにして正規の認証済み情報がクッキーとして記録されているクライアント12が

ら、その後Webサービスサーバ10にアクセスがあった場合には、Webサービスサーバ10はWeb認証サーバ16への問い合わせを行わない。図5は、かかるケースでのクライアント12とWebサービスサーバ10との間の通信を説明する通信シーケンス図である。

【0039】同図に示すように、クライアント12のユーザがWebサービスサーバ10に対するサービスを要求するURLを入力すれば(S201)、クライアント12にてそのURLをインターネットに送出する(S202)。この際、クライアント12には既にユーザ認証済みの旨のクッキーが記録されており、Webサービスサーバ10に送信されるURLにはその記録されたクッキーの内容が含まれる。その後、Webサービスサーバ10にてアクセス可否の確認が行われる(S203)。

【0040】そして、このケースのアクセスでは、上述した第2段階でのアクセス可否チェックにおいて必要なクッキーを備えているアクセスであると判断されるため、ユーザ所望のWebページに関するデータが正常にクライアント12に送信される(S204)。そして、クライアント12では受信したWebページを解釈してディスプレイ表示を行う。

【0041】なお、以上説明した認証システムは種々の変形実施が可能である。

【0042】たとえば、ユーザ認証済みの旨を表すクッキーにはそのユーザ認証の有効期限を表す情報を設定するようにしてもよい。こうすれば、Webサービスサーバ10はクライアント12からユーザ認証済みの旨を表すクッキーを受け取ったとしても、それが有効期限を過ぎたものであれば、必要に応じて、再びWeb認証サーバ16にアクセスしてユーザ認証を行うようクライアント12に要求することができる。

【0043】また、上記説明では、クライアント12、サービスサーバ、認証サーバがインターネットにされたものであり、それらがHTTPプロトコルに従うものであることを前提にしたが、本発明はプロトコルやネットワークの形態によらず、必要な構成を備えるすべてのネットワーク形態に適用可能なものである。

【0044】

【発明の効果】以上説明したように、本発明によればサービスサーバと認証サーバとの間での直接アクセスを廃し、ユーザ認証をクライアントと認証サーバとの間で直接に行わせるようにしたので、サービスサーバと認証サーバとの相互依存関係を少なくすることができる。このため、認証サーバの汎用性を高めて複数のサービスサ

バで該認証サーバを共用することが可能となる。

【0045】また、本発明によれば、認証サーバが認証済み情報をクライアントに送信する際にリダイレクト要求情報を併せてクライアントに送信するようにしたので、クライアントからサービスサーバへ再度アクセスする際のタイミングを認証サーバから提供することができる。この結果、たとえばクライアント12はこのリダイレクト要求情報の受信をトリガとして再びサービスサーバへアクセスすることが可能となる。

【0046】また、本発明によれば、クライアントがサービスサーバからリダイレクト要求情報を受信した場合にクライアントが自動的に認証サーバにアクセスするようにしたので、クライアントのユーザが特段の操作をすることなくユーザ認証を進めることができる。

【0047】また、本発明によれば、クライアントが認証サーバからリダイレクト要求情報を受信した場合にクライアントが自動的にサービスサーバにアクセスするようにしたので、ユーザ認証を無事に終えたクライアントのユーザが特段の操作をすることなく再びサービスサーバにアクセスすることができる。

【0048】また、本発明によれば、クライアントが既に認証済み情報を受け取っている場合、サービスサーバへのアクセスの際にその認証済み情報を該サービスサーバに送信するようにしたので、サービスサーバ側でのクライアントがユーザ認証に成功したものであることを知ることができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態に係る通信システムの全体構成を示す図である。

【図2】 本発明の実施の形態に係るWebサービスサーバを通信システムの全体構成とともに示す図である。

【図3】 本発明の実施の形態に係るWeb認証サーバの構成を示す図である。

【図4】 WebサービスサーバからWeb認証サーバへの問い合わせの様子を説明する通信シーケンス図である。

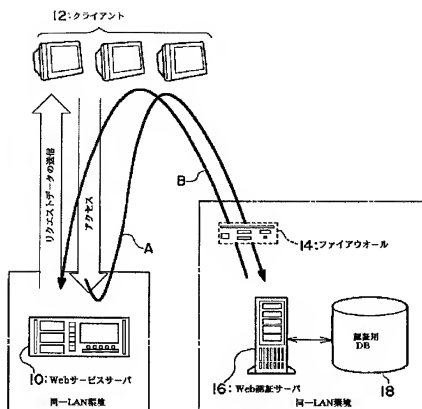
【図5】 ユーザ認証を正常に終えたクライアントとWebサービスサーバとの通信を説明する通信シーケンス図である。

【図6】 従来技術に係るユーザ認証の仕組みを説明する図である。

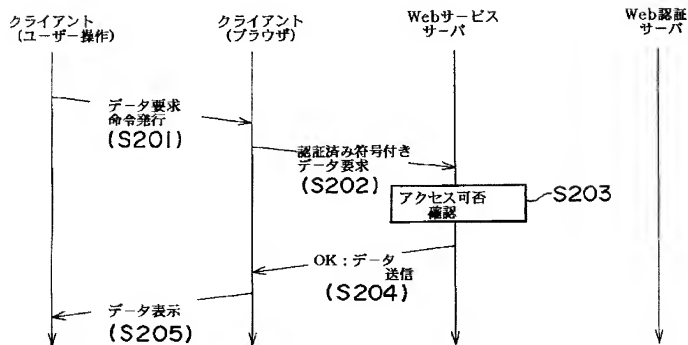
【符号の説明】

10 Webサービスサーバ、12 クライアント、16 Web認証サーバ、18 認証用データベース。

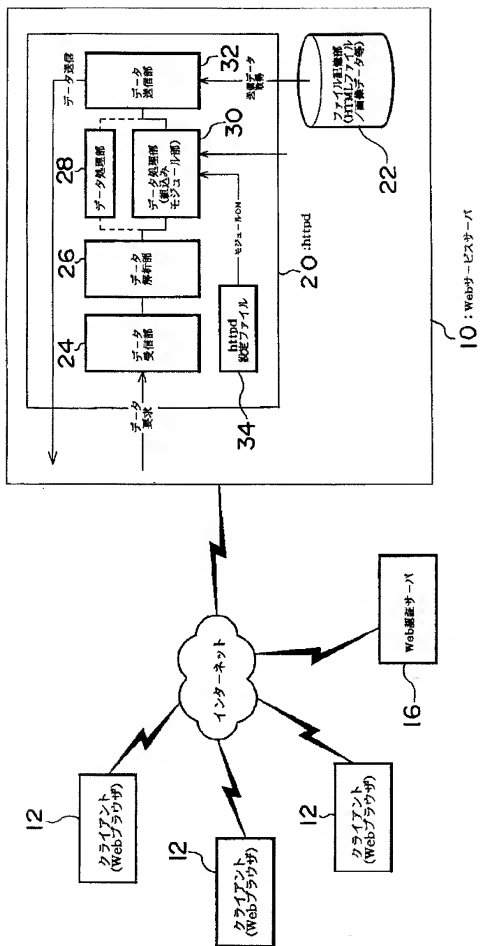
【図1】



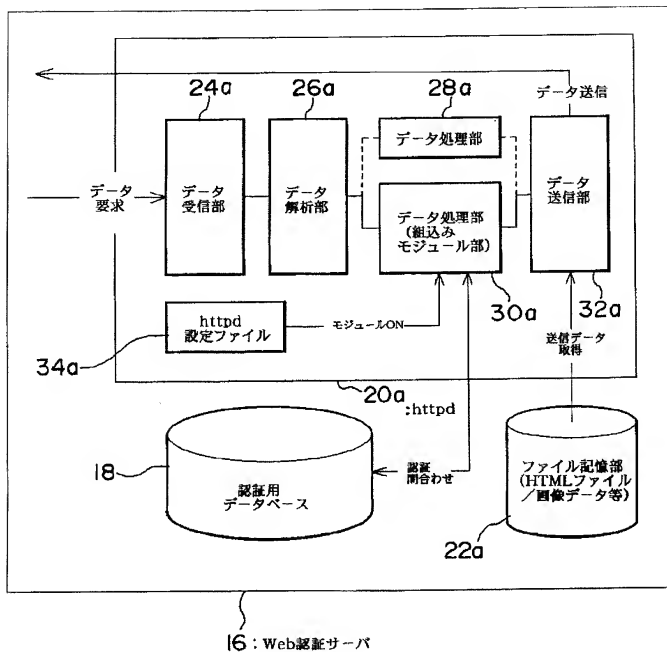
【図5】



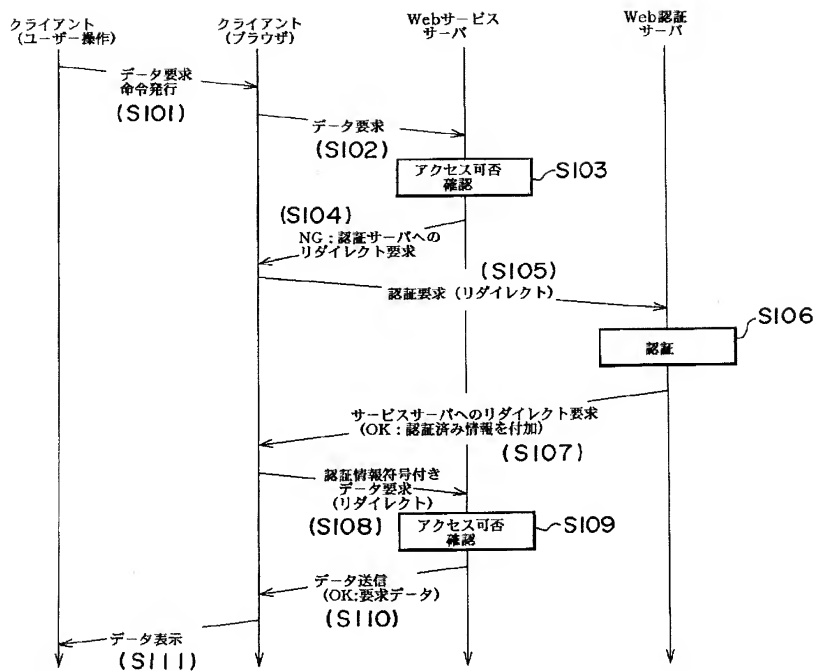
【図 2】



【図3】



【図4】



【図6】

